WATSON FARLEY
&
WILLIAMS

BRIEFING

GDPR, PDPB AND M&A TRANSACTIONS IN THAILAND

JULY 2018

- THE IMPACT OF GDPR AND PDPB ON CROSS-BORDER M&A TRANSACTIONS IN THAILAND
- THE REGULATORY AND COMPLIANCE ISSUES WHICH SHOULD BE ADDRESSED IN EACH STAGE OF AN M&A TRANSACTION

This briefing should be read in conjunction with our briefing "GDPR and PDPB: what do you need to know" of July 2018.

In this briefing, we consider the impact of GDPR and PDPB on cross-border M&A transactions.

Companies and individuals contemplating an M&A transaction, including preliminary due diligence ("DD"), must contend with increasing amounts of data and levels of detail of said data. This increase has been assisted and accelerated by technology and the enhanced speed of data processing. In some sectors, such as technology and healthcare and in consumer-facing industries and companies, the volume of data increases exponentially from one deal to the next.

The implementation of GDPR and the likely introduction of PDPB will increase the regulatory and compliance issues which the parties must address in an M&A transaction.

"THE TERMS OF ANY NDA WILL BE SUBJECT TO GDPR AND PDPB, PARTICULARLY THE RIGHTS OF THE SUBJECT OF THE DATA UNDER GDPR."

"COMPLIANCE WITH THESE REQUIREMENTS IS LIKELY TO MAKE DD A MORE TIME CONSUMING AND COMPLEX TASK."

"BUYERS SHOULD CONSIDER THE EXTENT TO WHICH THE PURCHASE PRICE SHOULD REFLECT BREACHES OF GDPR AND/OR PDPB."

Initial stages and DD

The initial stages of the transaction will typically revolve around the overall commercial terms of the transaction. Assuming the parties proceed from initial discussions to more focused negotiations, the level of detail in the data to be disclosed increases significantly, typically in tandem with increasingly focused and specific terms.

Where the target company agrees to disclose certain information or make part of its records available to the buyer, this is typically addressed by a non-disclosure or confidentiality agreement ("NDA"). Neither GPPR nor PDPB have any direct impact on the contents or operation of an NDA. However, their impact should be addressed in the terms and scope of the NDA, particularly the following:

- Whether the target company has the right to disclose the data and disclosure by it is in compliance with GDPR and any other applicable laws and regulations;
- Steps to protect the data, including a designated data controller;
- Use of the data only for stated purposes, where those purposes demonstrate the legitimate interest of the recipient or data controller;
- The location/s of the data; and
- For data in the EU, an agreement on the transfer of the data out of the EU.

The terms of any NDA will be subject to GDPR and PDPB, particularly the rights of the subject of the data under GDPR, including the rights of rectification, removal and restrictions on processing.

Before entering into an NDA, the parties should carefully consider the nature and scope of the data to be disclosed. The target company should consider the extent to which the disclosure of the data falls within the permitted categories under GDPR, particularly where disclosure is to give effect to a contract and where it is in the legitimate interest of the buyer and/or data controller. Data which falls outside these categories should be anonymised and any data which could identify an individual or individuals, and would then be in breach of GDPR, should be reviewed and their relevance to the DD or stage of the transaction carefully considered. Under PDPB, where the disclosure of data would not constitute a legitimate purpose of the data controller or buyer, prior written consent is required to the disclosure of personal data.

Compliance with these requirements is likely to make DD a more time consuming and complex task, particularly if the data must be more thoroughly and closely reviewed and considered before being disclosed. These issues should be addressed before and during the drafting of an NDA.

Negotiating the Sale and Purchase Agreement ("SPA")

The impact of GDPR and PDPB should also be considered in the context of negotiating the terms of the SPA. Buyers should consider the extent to which the purchase price should reflect breaches of GDPR and/or PDPB and whether the purchase price should be divided into instalments to mitigate the risk of fines and penalties imposed after completion arising from a breach of GDPR and/or PDPB by the target company prior to completion.

If the preliminary, pre-SPA DD has been completed and the transaction contemplates more detailed and thorough DD after the SPA is signed, a further NDA may be required to the extent that the critical issues are not addressed in the NDA for the pre-SPA DD.

"DATA CONTROLLERS WILL NEED TO CAREFULLY CONSIDER THE EXTENT TO WHICH DISCLOSURE OF PERSONAL DATA MEETS THE LEGITIMATE PURPOSE TEST IN THE CONTEXT OF THE TRANSACTION, FAILING WHICH PRIOR WRITTEN CONSENT TO DISCLOSURE WILL BE REQUIRED."

For the target, it is important to ensure that only data which meet the tests of legitimate interest and/or give effect to a contract are disclosed. The timing of the disclosure in the transaction is also a key factor and consideration should be given to disclosing data as late in the process as possible. This should also be balanced with the requirement to notify individuals in accordance with articles 13 and 14 of GDPR. Assuming the text of PDPB is not amended prior to coming into force, data controllers will need to carefully consider the extent to which disclosure of personal data meets the legitimate purpose test in the context of the transaction, failing which prior written consent to disclosure will be required. The time to obtain this consent and the consequences of a refusal would then need to be factored into the transaction timeline.

This is likely to be a critical issue in relation to customers, suppliers, employees, directors and shareholders.

For DD after the SPA is signed, the target company should ensure that it can demonstrate to the buyer that it complies with GDPR and/or PDPB. This will include that it is legally entitled to hold and disclose the data, it has a designated data protection officer, it has agreements with suppliers, customers and other parties to protect the handling of any personal data and to ensure that any data provided to these parties complies with GDPR and/or PDPB. The target company should also be prepared to disclose details of its data protection procedures and protocols, including potentially details of cyber risk insurance.

Buyers will need to undertake their own investigations into compliance with GDPR and/or PDPB by the target and satisfy themselves as to the level of compliance by the target.

"A CRITICAL FACTOR WILL BE RESTRICTING ACCESS TO THE DATA ROOM TO DESIGNATED INDIVIDUALS AND ENSURING THAT DETAILED AND COMPLETE RECORDS OF ALL ACCESS ARE GENERATED."

Where the parties agree to use a data room for DD and other disclosure during the transaction, this will also be subject to the provisions of GDPR and/or PDPB. Data rooms are increasingly outsourced to third parties. Where the data room is outsourced to a third party, it will be necessary to ensure that the third party complies with GDPR and/or PDPB, including a review of the terms and conditions on which the data room is provided and operated. A critical factor will be restricting access to the data room to designated individuals and ensuring that detailed and complete records of all access are generated and retained, particularly in the context of a request by a subject individual under GDPR for details of the processing of personal data and/or to restrict the processing of data in relation to that individual.

Post-transaction data processing and use

Where the transaction will result in the transfer of personal data or new uses or applications of personal data, the parties will need to ensure that this complies with GDPR and/or PDPB. This is particularly in the context of whether notification to the data subject or their consent is required for any post-transaction processing or use of their personal data. Buyers will need to assess the impact of the transaction on personal data held and processed by the target company and how they will process, store and protect the data after the transaction has been completed.

"NEGOTIATING REPRESENTATIONS AND WARRANTIES WILL NOW NEED TO ADDRESS COMPLIANCE WITH GDPR AND/OR PDPB AND ENSURE THAT THE CONSEQUENCES OF A BREACH ARE BORNE BY THE APPROPRIATE PARTY."

"BUYERS SHOULD BE REQUIRING REPRESENTATIONS AND WARRANTIES BY THE TARGET IN RELATION TO COMPLIANCE WITH GDPR AND/OR PDPB."

"IMPORTANT TO ASSESS THE EXTENT TO WHICH W&I INSURANCE IS AVAILABLE FOR THE CONSEQUENCES OF A BREACH OF GDPR AND/OR PDPB."

Representations and warranties

Negotiating representations and warranties can often be one of the more challenging aspects of an M&A transaction. These negotiations will now need to address compliance with GDPR and/or PDPB and ensure that the consequences of a breach are borne by the appropriate party. As noted above, this may need to be reflected in the structure of the payment of the purchase price.

Buyers should be requiring representations and warranties by the target in relation to compliance with GDPR and/or PDPB. Given the relatively clearly defined requirements in GDPR and PDPB, the representations and warranties should provide a sufficient and appropriate level of detail to buyers, particularly in relation to data processing, protection and transmission and the designated data protection officer. The representations and warranties should also address any identified and/or disclosed shortcomings of the data processing, protection and transmission systems and procedures of the target and buyers may need to require a suitable and appropriate level of rectification as a condition precedent to completion.

The representations and warranties will also need to take into account the outcome of the DD. This may also merit consideration of indemnities by the target of the buyers to rectify any deficiencies in GDPR and/or PDPB compliance or breaches of GDPR and/or PDPB and in respect of fines and penalties.

For all parties, this may make warranty and indemnity insurance ("W&I Insurance") more attractive and provide a level of comfort and protection. It will be important to assess the extent to which W&I Insurance is available for the consequences of a breach of GDPR and/or PDPB. This is particularly in relation to breaches known to the target and/or disclosed in the DD, for which W&I Insurance cover can be excluded or only be available on a limited basis.

The availability and cost of W&I Insurance may have an effect on the nature and extent of the representations and warranties. Buyers will need to consider whether it would be preferable to have a contractual indemnity from the target, with the risk that the target's assets may not be sufficient to meet any indemnity, or to rely on the greater certainty of an insurer's assets and have to deal with issues of insurance cover for any claim.

In seeking W&I Insurance cover, the parties will need to accept and accommodate the requirements of the insurer, including their assessment of the transaction and the risks of a breach of the representations and warranties. In effect, this can add an additional step to the transaction and an additional layer of scrutiny.

Disclosure of relevant data to a prospective insurer and broker must also comply with GDPR and/or PDPB. This is particularly relevant where the prospective insurer and broker are provided with access to a data room and/or DD reports.

FOR MORE INFORMATION

Should you like to discuss any of the matters raised in this Briefing, please speak with a member of our team below or your regular contact at Watson Farley & Williams.

ALAN POLIVNICK
Partner
Bangkok

+66 2 665 7805
apolivnick@wfw.com

KULKANYA VORAWANICHAR
Senior Associate
Bangkok

+66 2 665 7839
kvorawanichar@wfw.com

NICHAREE MUSIKAPRAPHAN
Associate
Bangkok

+66 2 665 7840
nmusikapraphan@wfw.com

Publication code number: 83537469v1